EA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/034,485	12/28/2001	Jong-Uk Choi	30360/37968	2206

4743 7590 09/13/2005

MARSHALL, GERSTEIN & BORUN LLP
233 S. WACKER DRIVE, SUITE 6300
SEARS TOWER
CHICAGO, IL 60606

EXAMINER	
BAYAT, BRADLEY B	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 09/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/034,485	CHOI ET AL.	
	Examiner	Art Unit	
	Bradley B. Bayat	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

This communication is in response to amendment filed on June 13, 2005.

- Claims 4, 6, 7, 11 15, 16 and 19 have been amended,
- Claims 1-19 remain pending.

Response to Arguments

Applicant's arguments filed in the above noted response have been fully considered but they are not persuasive. Applicant's arguments are addressed in order of appearance in the response and do not impart importance based on the sequence of responses as follows:

Applicant argues that the cited reference England et al. (20020012432 A1) fails to disclose a "user application tool installed in a user terminal, the user application being structured to create a unique user key using unique system information of the user terminal (response p.6)."

The "authoring tool" described in England is an example of one application tool installed on a user terminal [0074]. Moreover, England's various embodiments that comprehensively and dynamically perform secure digital rights management functions, a black box can is also implemented on a device to perform security and trust functions [0102-0103, 0159, 0173-0183]. In fact, applicant's main contention revolves around the portion of the claim wherein a unique key is created based on the user terminal system information (response pp. 6-9).

As applicant is aware, it is common knowledge in the computer and cryptographic arts that every CPU is capable of performing cryptographic functions, such as signing, encrypting, decrypting and authenticating. A CPU manufacturer equips a CPU with a pair of public and private keys that is unique to the CPU. The private key is never revealed and often used for responding to challenges from a content provider. In addition, a manufacturer also issues a

signed certificate wherein upon creation of the key pair onto the CPU, it has then destroyed its own knowledge of the private key. Therefore, only the CPU knows the private key. Furthermore, the CPU has an internal software identity register, which contains the identity of an authenticated operating system, wherein the boot block uniquely determines and identifies the user operating system (applicant is invited to review the references incorporated in the cited art and Handbook of Applied Cryptography by Menezes et al. for a better understanding of encryption techniques). Therefore, applicant's contention that such a broad limitation that uniquely identifies a user system can overcome the cited reference is clearly not persuasive. See England paragraphs 0050, 0079, 0107, 0120, 0138-0141.

Applicant also argues that the decryption in the license is encrypted and that none of the keys are created by the DRM system (response p.7). Applicant is directed to England paragraphs 0047, 0060, 0107, 0120, 0128, and 0186. Furthermore, the distinction as to location of key creation is not relevant in a distributed computing environment wherein each of the functions as claimed can be either accomplished by modules or software or hardware components.

Applicant further contends that England does not describe public/private key pairs made using the device (response p.8). See England paragraphs [0079, 0178-181] and response to arguments above. As noted above, the private key is unique to the device, unlike a public key.

As to the method claims of 6-9, applicant indicates that the comparison and matching feature is not disclosed by England (response p.8). England discloses a comparison mechanism in paragraphs 0077 and 0170. Without a filter/search/comparison/matching mechanism, neither the cited reference nor the claimed subject matter would be able to determine and validate access to protected content.

As per applicant's repeated argument regarding a unique terminal ID key, applicant is directed to the arguments noted above (pp. 8-9). In addition, applicant is directed to paragraphs 0088, 0096, 0127, 0137-0141 and 0204-0207 for further clarification. It is important to note that applicant further discloses user registration and company upload/download process to accomplish the authentication process, which can be accomplished without transmitting unique system information as argued above (see applicant's specification paragraphs 0053-0061).

As per claim 16-19, applicant argues that a document key/read/file storing mechanism is not disclosed in England (response p.10). Applicant is directed to review England paragraphs 0063-0074. Thus, England discloses a more comprehensive document storing and filtering mechanism than purported by applicant.

Claim Rejections - 35 USC § 102

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by England et al. (hereinafter England), US 2002/0012432 A1.

As per the following claims, England discloses:

1. A digital information security system comprising: a user application tool installed in a user terminal, the user application tool being structured to create a unique user key using unique system information of the user terminal; a data storage unit for storing user information and digital information; and a user management tool installed in a server, the user management tool being structured to receive the unique user key created by the user application tool, the user management tool being structured to store the received unique user key in the data storage unit,

the user management tool being structured to compare the stored unique user key with a unique user key provided from the user application tool of a user currently being subjected to authentication (¶10-21).

2. The digital information security system as claimed in claim 1, further comprising a history manager for managing user access and use history (¶78, 107).

3. The digital information security system as claimed in claim 1, wherein the unique system information includes at least one of unique CPU (Central Processing Unit) information, unique HDD (Hard Disk Drive) information, and serial number information of the user terminal (¶58, 77, 137).

4. The digital information security system as claimed in claim 1, further comprising a rule establishing unit for establishing a established rule according to a user rule previously established for the stored digital information, wherein the user application tool transmits information on the user rule during download of the digital information to the user, wherein upon downloading the digital information, the user application tool determines whether to output the downloaded digital information according to the established rule (¶290-292).

5. The digital information security system as claimed in claim 4, wherein said digital information includes an encrypted user requested digital file and a digital file decoding key using said unique user key and said rule information (figures 9-11 and associated text).

6. A digital information security method comprising: reading a first unique user key created using unique system information of a user terminal when a sever is accessed by a user; comparing the first unique user key with a second unique user key included in previously stored user information for the user, to authenticate whether the user is an authorized user; encrypting a file uploaded by the authorized user using a preset encryption key, and storing the encrypted file as digital information; and encrypting a decoding key for the corresponding digital information using the second unique user key included in the user information, and downloading the encrypted decoding key along with the associated digital information in response to a digital information download request of the authorized user (¶274-290).

7. The digital information security method as claimed in claim 6, further comprising the step of decoding the digital information by decoding the encrypted decoding key for the digital information downloaded from the user terminal using the first unique user key created from the unique system information (¶185-187)

8. The digital information security method as claimed in claim 6, wherein the downloading includes said encrypted digital file and said decoding key of said encrypted digital file and rule information on use authority (¶112).

9. The digital information security method as claimed in claim 6, further comprising: transmitting to the user a program for creating and transmitting the first unique user key using

the unique system information of the user terminal when the user is unregistered, so as to allow the user to install the program in the user terminal; and registering by the installed program the corresponding user using the first unique user key (¶173-183).

10. A digital information security method comprising the steps of: creating a unique user key at a user terminal using unique system information of the user terminal; decoding an encrypted decoding key included in the digital information at the user terminal using the created unique user key; and decoding the digital information using the decoded decoding key, wherein the encrypted decoding key cannot be decoded when the key used for decoding the encrypted decoding key is not identical to the created unique user key (¶185-187).

11. A digital information security system comprising: a key management service module installed in a user system, the key management service module being structured to encrypt user information including a unique user ID created based on system information of a corresponding user from a user application tool installed in a system of the user, and storing the encrypted user information; a document management service gateway structured to create a document key for the file when a file is uploaded from the user store the created document key, and encrypt a corresponding file using the created document key; a document distribution service module structured to create an encrypted download file including information on an output rule of the file in a predetermined user environment when downloading the file to the user; and a web server structured to transmit information on the file uploaded through the Internet by the user to the document management service gateway so that the document management service gateway

encrypts the file, and transmit, upon receipt of a file download request from the user, information on the request to the document distribution service module so that the document distribution service module creates an encrypted download file for the file (figures 5-9 and associated text).

12. The digital information security system as claimed in claim 11, wherein the user application tool is structured to create the unique user ID and transmit the user information during initial installation and upgrade of the user system (¶173-183).

13. The digital information security system as claimed in claim 11, wherein the user application tool includes a document viewer module structured to call a plurality of document edition software programs, output the called programs in a predetermined window, and allow the user to execute the document edition software programs (¶272-292).

14. The digital information security system as claimed in claim 13, wherein the document viewer module is structured to allow the user to execute the document edition software program on the window, and determine whether to perform a predetermined execution control operation including an operation of saving and printing a predetermined file according to predetermined rule information and user information for the file downloaded during execution of the document edition software program (¶48-66).

15. The digital information security system as claimed in claim 11, wherein communication among the document key management service module, the document management service gate,

the document distribution service module and the web server is performed through TCP/IP (Transmission Control Protocol/Internet Protocol) (figure 12 and associated text).

16. A digital information security method in a digital information security system including a documents key management service module for managing user information including a unique user ID created based on system information of a user, a document management service gateway for encrypting a corresponding file by creating a document key for an uploaded file, a document distribution service module for creating an encrypted download file including information on an output rule of a file to be downloaded, and a web server for performing a file uploading/download operation with the user through the Internet, transmitting information on an uploaded file to the document management service gateway and transmitting information on a download request to the document distribution service module, the method comprising the steps of: transmitting by the web server information on the uploaded file to the document management service gateway; reading by the document management service gateway the uploaded file by accessing a position where the file is actually uploaded from the server, using the information on the uploaded file; creating a document key for the read file in a predetermined decoding method, and storing the created document key along with the corresponding file information; encrypting the file using the created document key; storing the encrypted file in a predetermined folder; and informing the web server that processing the uploaded file is completed (see above; ¶108-120).

17. The digital information security method as claimed in claim 16, further comprising the steps of: upon receipt of a file download request, transmitting by the web server information on a

download-requested file to the document distribution service module; accessing by the document distribution service module a corresponding encrypted file using the information on the download-requested file; creating an encrypted download document file matched with an authority of the user based on user information of the user and information on the document key for the document and the output rule; storing the created encrypted download file in a download position; and informing the web server that processing the download-requested file is completed (¶114-158).

18. The digital information security method as claimed in claim 16, wherein the information on the output rule includes a save authority which is a rule indicating whether the user can save the download document file in a user terminal of the user, a print authority which is a rule indicating possibility and number of printing the download document file, an available term authority indicating a rule for an available term of the download document file, and an assignment authority indicating a rule for assignment of the download document file (¶117, 142).

19. The digital information security method as claimed in claimed 17, said creating an encrypted download document file includes combining said rule information on said authority with said decoding key of said encrypted file and encrypting said rule information and said decoding key using said unique user ID and combining combined said rule information and decoding key with said encrypted download document file (¶185-189).

Although the Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action, the specified citations are merely representative of the teachings in the art as applied to the specific limitations within the individual claim. Since other passages and figures may apply to the claimed invention as well, it is respectfully requested that the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- US Patent Number 5,892,900 to Ginter et al.
- US Patent 6,330,670 B1 to England et al.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bradley B. Bayat whose telephone number is 571-272-6704. The examiner can normally be reached on Tuesday - Friday 8 a.m.-6:30 p.m. and by email: bradley.bayat@uspto.gov. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached regarding urgent matters at 571-272-6712.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Or faxed to:

(571) 273-8300 - Official communications; including After Final responses.

(571) 273-6704 - Informal/Draft communications to the examiner.

bbb